

Abstract

Device and method for performing operations at a variable speed

A processor comprises a computation unit for performing an operation at a speed and a state unit, which has a state which changes in response to execution of an operation by the computation unit, the speed of the computation unit being controlled according to the state of the state unit. The state unit can e.g. be a capacitor or a unit with a thermal capacitance and controlling the speed of the computation unit can e.g. be effected via the frequency of a clock rate. In cryptographic applications the state unit is preferably so designed that the speed decreases when an operation is executed.